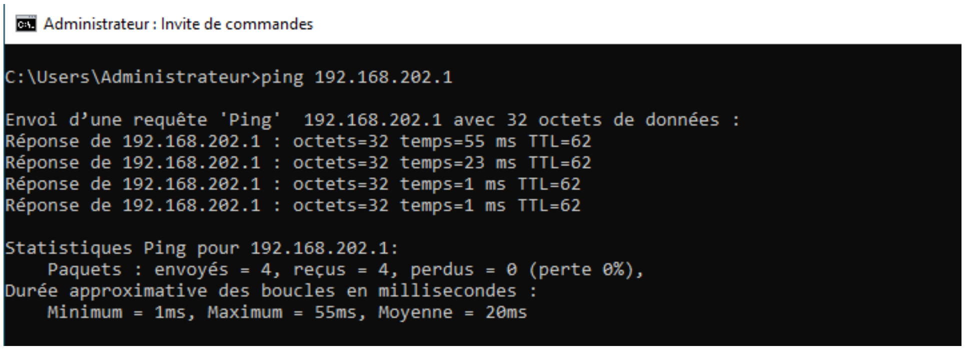
Enzo Juillard 2ESGI4

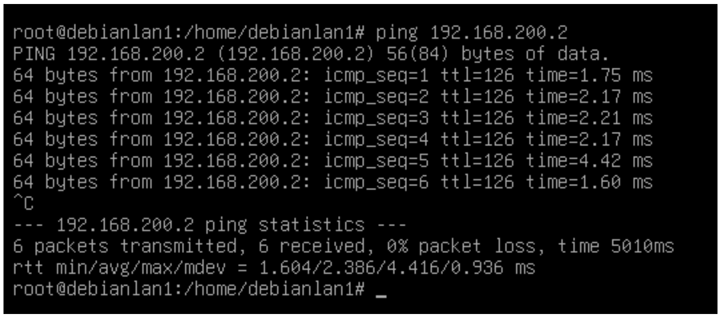
Récap Infra pfSense

Communications :

Windows Server (Lan 1) vers Debian (Lan 2) et inversement

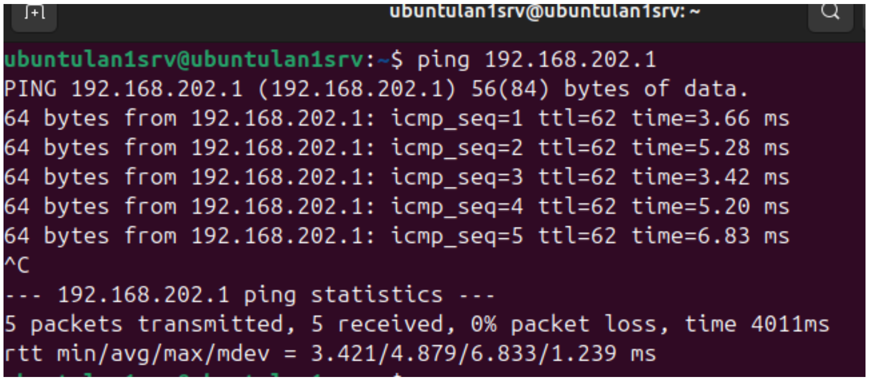


```
C:\Users\Administrateur>ping 192.168.202.1

Envoi d'une requête 'Ping'  192.168.202.1 avec 32 octets de données :
Réponse de 192.168.202.1 : octets=32 temps=55 ms TTL=62
Réponse de 192.168.202.1 : octets=32 temps=23 ms TTL=62
Réponse de 192.168.202.1 : octets=32 temps=1 ms TTL=62
Réponse de 192.168.202.1 : octets=32 temps=1 ms TTL=62

Statistiques Ping pour 192.168.202.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 55ms, Moyenne = 20ms
```

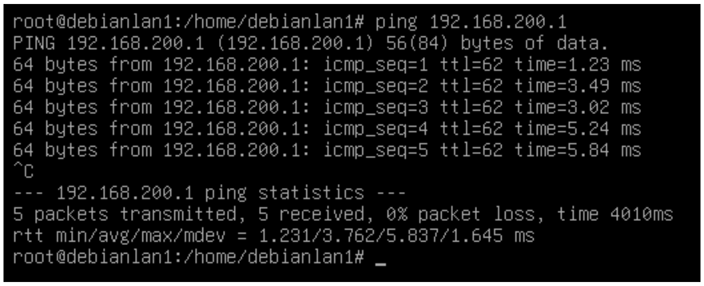


```
root@debianlan1:/home/debianlan1# ping 192.168.200.2
PING 192.168.200.2 (192.168.200.2) 56(84) bytes of data.
64 bytes from 192.168.200.2: icmp_seq=1 ttl=126 time=1.75 ms
64 bytes from 192.168.200.2: icmp_seq=2 ttl=126 time=2.17 ms
64 bytes from 192.168.200.2: icmp_seq=3 ttl=126 time=2.21 ms
64 bytes from 192.168.200.2: icmp_seq=4 ttl=126 time=2.17 ms
64 bytes from 192.168.200.2: icmp_seq=5 ttl=126 time=4.42 ms
64 bytes from 192.168.200.2: icmp_seq=6 ttl=126 time=1.60 ms
^C
--- 192.168.200.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 1.604/2.386/4.416/0.936 ms
root@debianlan1:/home/debianlan1# _
```

Ubuntu (Lan 1) vers Debian (Lan 2) et inversement

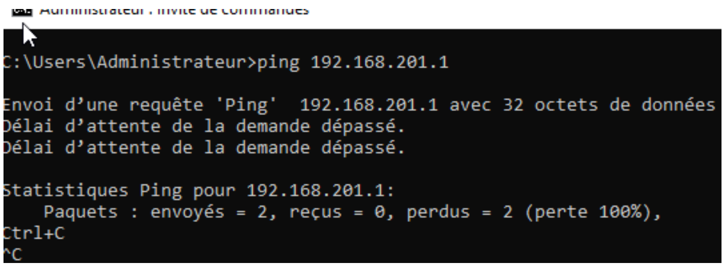


```
ubuntulan1srv@ubuntulan1srv:~$ ping 192.168.202.1
PING 192.168.202.1 (192.168.202.1) 56(84) bytes of data.
64 bytes from 192.168.202.1: icmp_seq=1 ttl=62 time=3.66 ms
64 bytes from 192.168.202.1: icmp_seq=2 ttl=62 time=5.28 ms
64 bytes from 192.168.202.1: icmp_seq=3 ttl=62 time=3.42 ms
64 bytes from 192.168.202.1: icmp_seq=4 ttl=62 time=5.20 ms
64 bytes from 192.168.202.1: icmp_seq=5 ttl=62 time=6.83 ms
^C
--- 192.168.202.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 3.421/4.879/6.833/1.239 ms
```



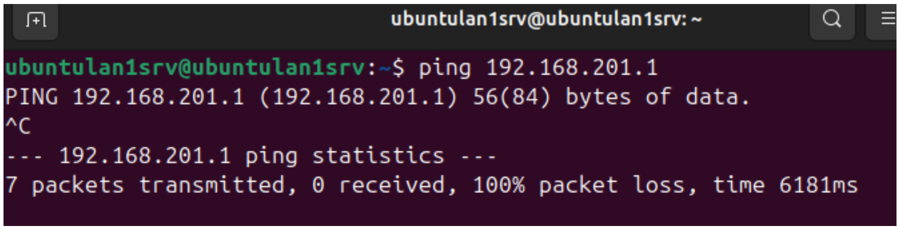
```
root@debianlan1:/home/debianlan1# ping 192.168.200.1
PING 192.168.200.1 (192.168.200.1) 56(84) bytes of data.
64 bytes from 192.168.200.1: icmp_seq=1 ttl=62 time=1.23 ms
64 bytes from 192.168.200.1: icmp_seq=2 ttl=62 time=3.49 ms
64 bytes from 192.168.200.1: icmp_seq=3 ttl=62 time=3.02 ms
64 bytes from 192.168.200.1: icmp_seq=4 ttl=62 time=5.24 ms
64 bytes from 192.168.200.1: icmp_seq=5 ttl=62 time=5.84 ms
^C
--- 192.168.200.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 1.231/3.762/5.837/1.645 ms
root@debianlan1:/home/debianlan1# _
```

Windows Server (Lan 1) vers Ubuntu (DMZ) => ne doivent pas communiquer ensemble



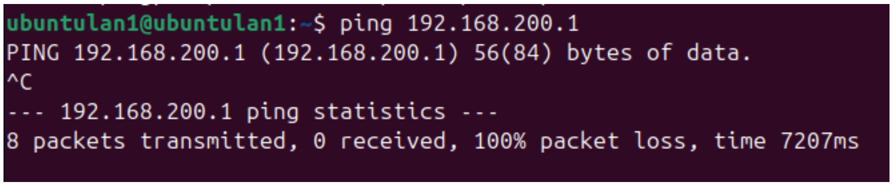
```
C:\Users\Administrateur>ping 192.168.201.1

Envoi d’une requête 'Ping'  192.168.201.1 avec 32 octets de données
Délai d’attente de la demande dépassé.
Délai d’attente de la demande dépassé.

Statistiques Ping pour 192.168.201.1:
    Paquets : envoyés = 2, reçus = 0, perdus = 2 (perte 100%),
Ctrl+C
^C
```

Ubuntu (Lan 1) vers Ubuntu (DMZ) => ne doivent pas communiquer ensemble



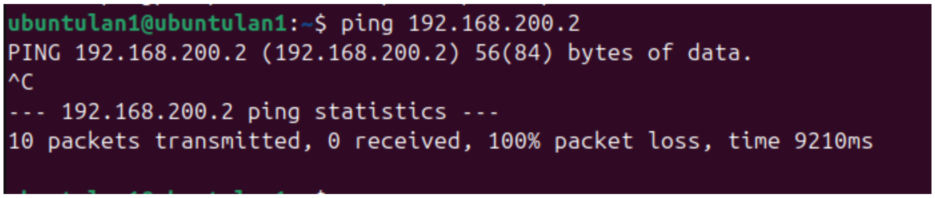
```
ubuntulan1srv@ubuntulan1srv:~$ ping 192.168.201.1
PING 192.168.201.1 (192.168.201.1) 56(84) bytes of data.
^C
--- 192.168.201.1 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6181ms
```

Ubuntu (DMZ) vers Ubuntu (Lan 1) => ne doivent pas communiquer ensemble



```
ubuntulan1@ubuntulan1:~$ ping 192.168.200.1
PING 192.168.200.1 (192.168.200.1) 56(84) bytes of data.
^C
--- 192.168.200.1 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7207ms
```

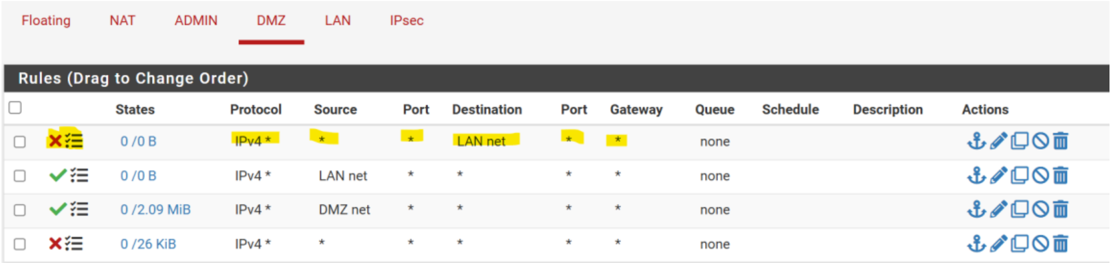
Ubuntu (DMZ) vers Windows Server (Lan 1) => ne doivent pas communiquer ensemble



```
ubuntulan1@ubuntulan1:~$ ping 192.168.200.2
PING 192.168.200.2 (192.168.200.2) 56(84) bytes of data.
^C
--- 192.168.200.2 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9210ms
```

règles que j'ai mis en place pour cela :

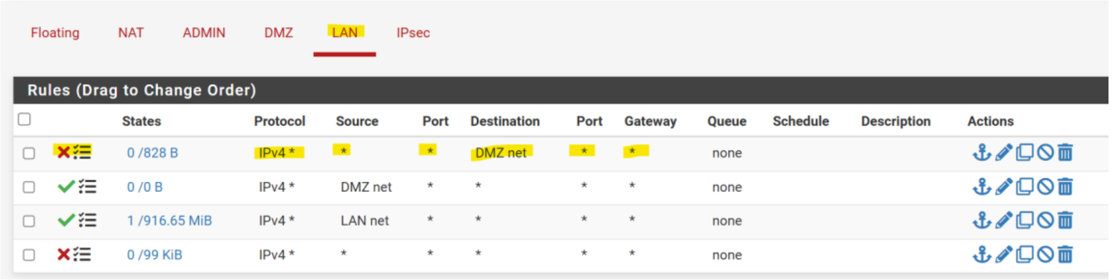
DMZ :



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗☰	0 /0 B	IPv4 *	*	*	LAN net	*	*	none			⚓✎⧉⊘🗑
□	✓☰	0 /0 B	IPv4 *	LAN net	*	*	*	*	none			⚓✎⧉⊘🗑
□	✓☰	0 /2.09 MiB	IPv4 *	DMZ net	*	*	*	*	none			⚓✎⧉⊘🗑
□	✗☰	0 /26 KiB	IPv4 *	*	*	*	*	*	none			⚓✎⧉⊘🗑

LAN 1 :

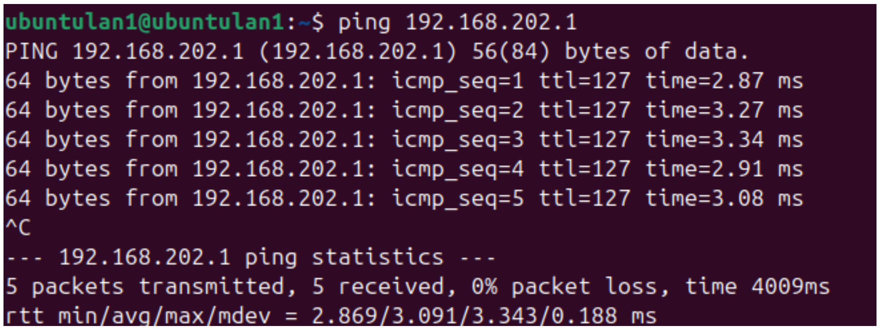


Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗☰	0 /828 B	IPv4 *	*	*	DMZ net	*	*	none			⚓✎⧉⊘🗑
□	✓☰	0 /0 B	IPv4 *	DMZ net	*	*	*	*	none			⚓✎⧉⊘🗑
□	✓☰	1 /916.65 MiB	IPv4 *	LAN net	*	*	*	*	none			⚓✎⧉⊘🗑
□	✗☰	0 /99 KiB	IPv4 *	*	*	*	*	*	none			⚓✎⧉⊘🗑

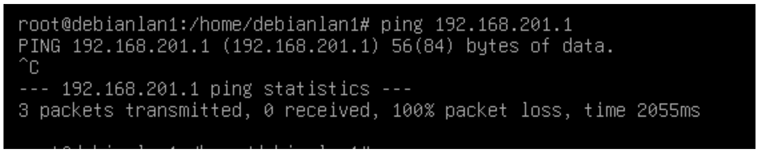
Communication entre Lan 2 et DMZ :

Ubuntu (DMZ) vers Debian (Lan 2)



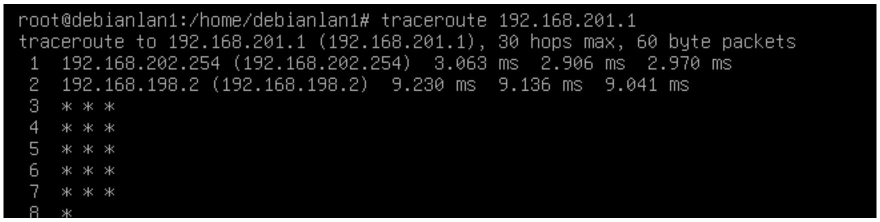
```
ubuntulan1@ubuntulan1:~$ ping 192.168.202.1
PING 192.168.202.1 (192.168.202.1) 56(84) bytes of data.
64 bytes from 192.168.202.1: icmp_seq=1 ttl=127 time=2.87 ms
64 bytes from 192.168.202.1: icmp_seq=2 ttl=127 time=3.27 ms
64 bytes from 192.168.202.1: icmp_seq=3 ttl=127 time=3.34 ms
64 bytes from 192.168.202.1: icmp_seq=4 ttl=127 time=2.91 ms
64 bytes from 192.168.202.1: icmp_seq=5 ttl=127 time=3.08 ms
^C
--- 192.168.202.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 2.869/3.091/3.343/0.188 ms
```

Debian (Lan 2) vers Ubuntu (DMZ)



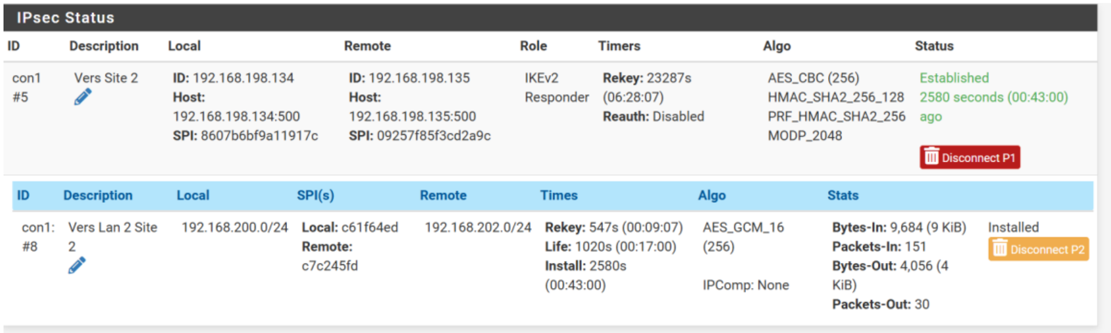
```
root@debianlan1:/home/debianlan1# ping 192.168.201.1
PING 192.168.201.1 (192.168.201.1) 56(84) bytes of data.
^C
--- 192.168.201.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2055ms
```

ne communiquent pas (j'ai pas trouvé pourquoi le seul indice c'est le traceroute) :



```
root@debianlan1:/home/debianlan1# traceroute 192.168.201.1
traceroute to 192.168.201.1 (192.168.201.1), 30 hops max, 60 byte packets
 1  192.168.202.254 (192.168.202.254)  3.063 ms  2.906 ms  2.970 ms
 2  192.168.198.2 (192.168.198.2)  9.230 ms  9.136 ms  9.041 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  *
```

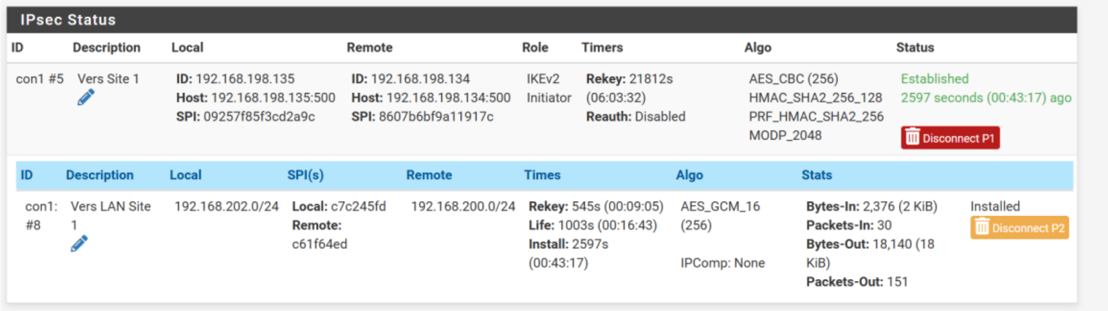
Config et preuves de connexions via l'ipSec (via les logs) :



IPsec Status

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #5	Vers Site 2	**ID:** 192.168.198.134 **Host:** 192.168.198.134:500 **SPI:** 8607b6bf9a11917c	**ID:** 192.168.198.135 **Host:** 192.168.198.135:500 **SPI:** 09257f85f3cd2a9c	IKEv2 Responder	**Rekey:** 23287s (06:28:07) **Reauth:** Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 2580 seconds (00:43:00) ago Disconnect P1

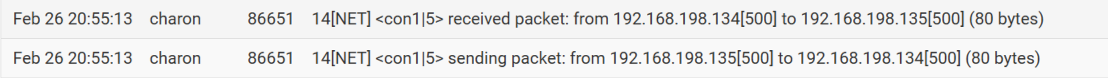
ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats	
con1: #8	Vers Lan 2 Site 2	192.168.200.0/24	**Local:** c61f64ed **Remote:** c7c245fd	192.168.202.0/24	**Rekey:** 547s (00:09:07) **Life:** 1020s (00:17:00) **Install:** 2580s (00:43:00)	AES_GCM_16 (256) IPComp: None	**Bytes-In:** 9,684 (9 KiB) **Packets-In:** 151 **Bytes-Out:** 4,056 (4 KiB) **Packets-Out:** 30	Installed Disconnect P2



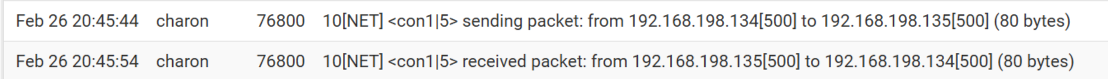
IPsec Status

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #5	Vers Site 1	**ID:** 192.168.198.135 **Host:** 192.168.198.135:500 **SPI:** 09257f85f3cd2a9c	**ID:** 192.168.198.134 **Host:** 192.168.198.134:500 **SPI:** 8607b6bf9a11917c	IKEv2 Initiator	**Rekey:** 21812s (06:03:32) **Reauth:** Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 2597 seconds (00:43:17) ago Disconnect P1

ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats	
con1: #8	Vers LAN Site 1	192.168.202.0/24	**Local:** c7c245fd **Remote:** c61f64ed	192.168.200.0/24	**Rekey:** 545s (00:09:05) **Life:** 1003s (00:16:43) **Install:** 2597s (00:43:17)	AES_GCM_16 (256) IPComp: None	**Bytes-In:** 2,376 (2 KiB) **Packets-In:** 30 **Bytes-Out:** 18,140 (18 KiB) **Packets-Out:** 151	Installed Disconnect P2



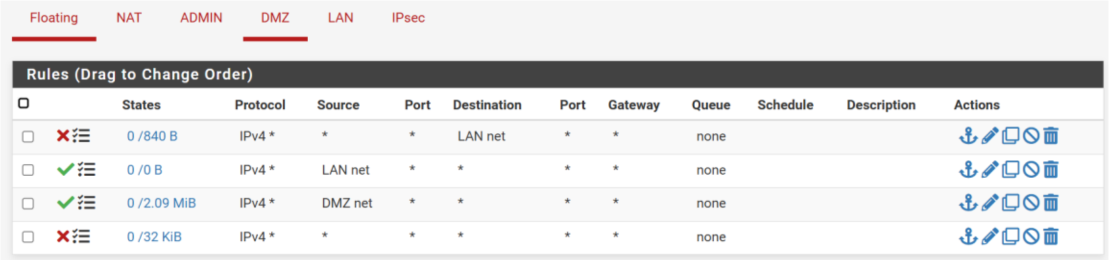
```
Feb 26 20:55:13   charon   86651   14[NET] <con1|5> received packet: from 192.168.198.134[500] to 192.168.198.135[500] (80 bytes)
Feb 26 20:55:13   charon   86651   14[NET] <con1|5> sending packet: from 192.168.198.135[500] to 192.168.198.134[500] (80 bytes)
```



```
Feb 26 20:45:44   charon   76800   10[NET] <con1|5> sending packet: from 192.168.198.134[500] to 192.168.198.135[500] (80 bytes)
Feb 26 20:45:54   charon   76800   10[NET] <con1|5> received packet: from 192.168.198.135[500] to 192.168.198.134[500] (80 bytes)
```

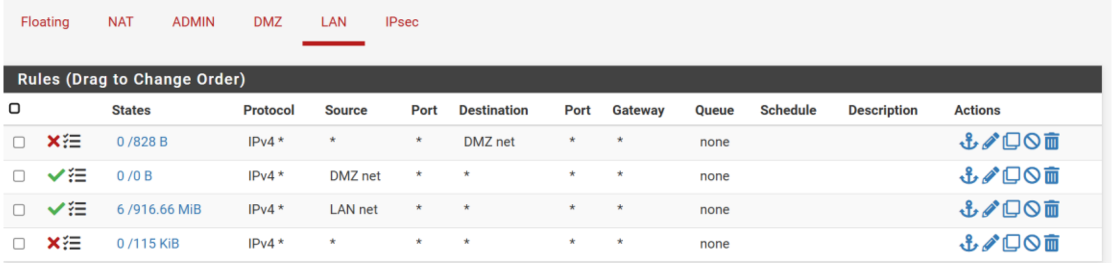
Voici mes règles selon les interfaces pour faire passer les paquets :

Site 1 :



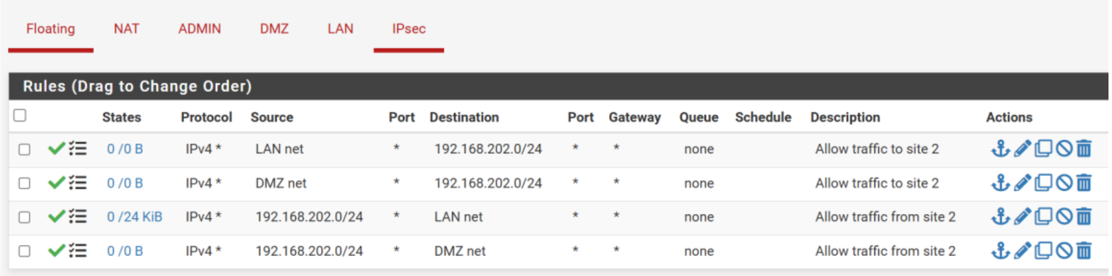
Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗	0 /840 B	IPv4 *	*	*	LAN net	*	*	none			
□	✓	0 /0 B	IPv4 *	LAN net	*	*	*	*	none			
□	✓	0 /2.09 MiB	IPv4 *	DMZ net	*	*	*	*	none			
□	✗	0 /32 KiB	IPv4 *	*	*	*	*	*	none			



Rules (Drag to Change Order)

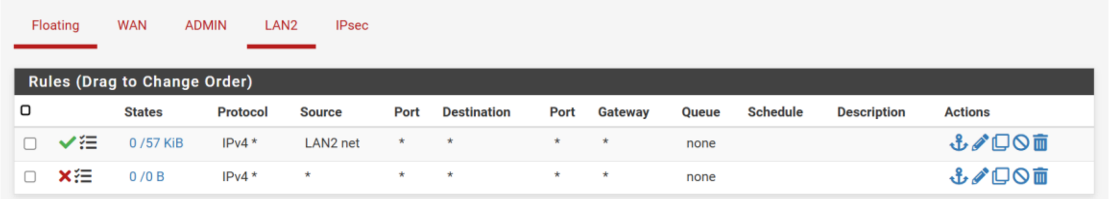
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗	0 /828 B	IPv4 *	*	*	DMZ net	*	*	none			
□	✓	0 /0 B	IPv4 *	DMZ net	*	*	*	*	none			
□	✓	6 /916.66 MiB	IPv4 *	LAN net	*	*	*	*	none			
□	✗	0 /115 KiB	IPv4 *	*	*	*	*	*	none			



Rules (Drag to Change Order)

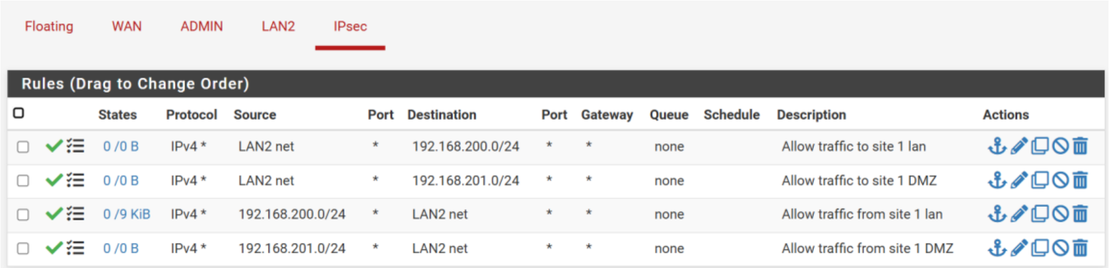
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /0 B	IPv4 *	LAN net	*	192.168.202.0/24	*	*	none		Allow traffic to site 2	
□	✓	0 /0 B	IPv4 *	DMZ net	*	192.168.202.0/24	*	*	none		Allow traffic to site 2	
□	✓	0 /24 KiB	IPv4 *	192.168.202.0/24	*	LAN net	*	*	none		Allow traffic from site 2	
□	✓	0 /0 B	IPv4 *	192.168.202.0/24	*	DMZ net	*	*	none		Allow traffic from site 2	

Site 2 :



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /57 KiB	IPv4 *	LAN2 net	*	*	*	*	none			
□	✗	0 /0 B	IPv4 *	*	*	*	*	*	none			



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /0 B	IPv4 *	LAN2 net	*	192.168.200.0/24	*	*	none		Allow traffic to site 1 lan	
□	✓	0 /0 B	IPv4 *	LAN2 net	*	192.168.201.0/24	*	*	none		Allow traffic to site 1 DMZ	
□	✓	0 /9 KiB	IPv4 *	192.168.200.0/24	*	LAN2 net	*	*	none		Allow traffic from site 1 lan	
□	✓	0 /0 B	IPv4 *	192.168.201.0/24	*	LAN2 net	*	*	none		Allow traffic from site 1 DMZ	